UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/057,043	01/25/2002	Ranga S. Ramanujan	1032-001US01	3446

28863 7590 02/23/2006

SHUMAKER & SIEFFERT, P. A.
8425 SEASONS PARKWAY
SUITE 105
ST. PAUL, MN 55125

EXAMINER	
GILLIS, BRIAN J	

ART UNIT	PAPER NUMBER
2141	

DATE MAILED: 02/23/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/057,043	RAMANUJAN ET AL.	
	Examiner	Art Unit	
	Brian J. Gillis	2141	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *28 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-17,27-30,35-46 and 51-56* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-17,27-30,35-46 and 51-56* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *25 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1, 3, 4, 6, 8, 27, 28, 30, 35, 37-39, 41-44, 51-53, and 56 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Chen et al (US Patent #6,353,593).

Claim 1 discloses a method comprising: establishing a packet tunnel having a source network address and a destination network address; detecting a network attack; selecting a new network address for at least one of the source network address and the destination network address upon detecting the network attack; and establishing a new packet tunnel using the new network address, wherein the new packet tunnel comprises two or more concatenated packet tunnels. Genty et al teaches of a tunnel between a source and destination (figure 7), an attack is detected (column 5, lines 48-52), a secondary tunnel can be established with different addresses (column 5, lines 63-67 – column 6, lines 1-6, 20-24), and a secondary tunnel is established (figure 7). It fails to teach of the new packet tunnel comprises two or more concatenated packet tunnels. Chen et al teaches of a virtual path connection (VPC) 38 which must be concatenated to the destination links in order for the virtual channel connections (VCCs) 36 carried by

VPC 38 to be routed on the destination links to their destination, (figure 1, column 4, lines 8-21).

Genty et al and Chen et al are analogous art because they are both related to data protection over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the concatenation in Chen et al with the system in Genty et al because an improved protection architecture is provided for virtual connections in a network (Chen et al, column 1, lines 33-45).

Claim 3 discloses the method of claim 1, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses. Genty et al further teaches the addresses are IP addresses (column 5, lines 1-5).

Claim 4 discloses the method of claim 1, wherein detecting a network attack comprises detecting an attack on an access link coupling a destination network device to a network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 6 discloses the method of claim 1, further comprising exchanging a set of available network addresses between a source network device originating the packet tunnel and a destination network device terminating the packet tunnel. Genty et al further teaches each device has a set of several addresses, which are exchanged to each device (column 5, lines 34-41).

Claim 8 discloses the method of claim 1, wherein establishing a new packet tunnel using the new network address further comprises: selecting an intermediate

network device; establishing a first packet tunnel that terminates on the intermediate network device; and establishing a second packet tunnel that originates from the intermediate network. Chen et al further teaches of the VPC must be concatenated to the destination links in order for the VCCs carried by VPC to be routed on the destination links to their destination, which forms a continuous packet tunnel from multiple concatenated tunnels with intermediate devices, when a new path is chosen the intermediate devices are inherently chosen during the route selection (column 2, lines 10-18, and 23-28).

Claim 27 discloses a method comprising: establishing virtual private network service including a packet tunnel having a source network address and a destination network address; detecting a network attack; and establishing new virtual private network service upon detecting the network attack, wherein the new virtual private network service comprises two or more concatenated packet tunnels. Genty et al teaches of a tunnel between a source and destination (figure 7), an attack is detected (column 5, lines 48-52), and a secondary tunnel is established (figure 7). It fails to teach of the new packet tunnel comprises two or more concatenated packet tunnels. Chen et al teaches of a virtual path connection (VPC) 38 which must be concatenated to the destination links in order for the virtual channel connections (VCCs) 36 carried by VPC 38 to be routed on the destination links to their destination, (figure 1, column 4, lines 8-21).

Genty et al and Chen et al are analogous art because they are both related to data protection over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the concatenation in Chen et al with the system in Genty et al because an improved protection architecture is provided for virtual connections in a network (Chen et al, column 1, lines 33-45).

Claim 28 discloses the method of claim 27, wherein establishing the new virtual private network service comprises: selecting an intermediate network device upon detecting the network attack; establishing a first packet tunnel from the source network address and terminating on the intermediate network device; and establishing a second packet tunnel originating from the intermediate network device and terminating at the destination network address. Chen et al further teaches of the VPC must be concatenated to the destination links in order for the VCCs carried by VPC to be routed on the destination links to their destination, which forms a continuous packet tunnel from multiple concatenated tunnels with intermediate devices, when a new path is chosen the intermediate devices are inherently chosen during the route selection (column 2, lines 10-18, and 23-28).

Claim 30 discloses the method of claim 27, wherein detecting a network attack comprises detecting an attack on an access link coupling a destination network device to a network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 35 discloses a system comprising a source device coupled to a network; and a destination device coupled to the network, wherein the source device and the destination device establish a packet tunnel having a source network address and a

destination network address and, upon detecting a network attack, select a new network address for at least one of the source network address and the destination network address and establish a new packet tunnel, wherein the new packet tunnel comprises two or more concatenated packet tunnels. Genty et al teaches of a tunnel between a source and destination, an attack is detected, and a secondary tunnel is established (column 5, lines 48-52, figure 7). It fails to teach of the new packet tunnel comprises two or more concatenated packet tunnels. Chen et al teaches of a virtual path connection (VPC) 38 which must be concatenated to the destination links in order for the virtual channel connections (VCCs) 36 carried by VPC 38 to be routed on the destination links to their destination, (figure 1, column 4, lines 8-21).

Genty et al and Chen et al are analogous art because they are both related to data protection over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the concatenation in Chen et al with the system in Genty et al because an improved protection architecture is provided for virtual connections in a network (Chen et al, column 1, lines 33-45).

Claim 37 discloses the system of claim 35, wherein the source network address and the destination network address comprise Internet Protocol (IP) addresses. Genty et al further teaches the addresses are IP addresses (column 5, lines 1-5).

Claim 38 discloses the system of claim 35, wherein the destination device and the source device comprise edge routers that couple local area networks to the network.

Genty et al further teaches the system can be accomplished by routers (column 3, lines 21-26).

Claim 39 discloses the system of claim 35, wherein the destination device detects an attack on an access link coupling the destination device to the network. Genty et al further teaches an attack can be detected on the network (column 5, lines 48-52).

Claim 41 discloses the system of claim 35, wherein the destination device and the source device exchange a set of available network addresses for the source network address and the destination network address of the packet tunnel. Genty et al further teaches each device has a set of several addresses, which are exchanged to each device (column 5, lines 34-41).

Claim 42 discloses the system of claim 35, wherein the destination device comprises a storage medium to store a set of available network addresses for use as the source network address and the destination network address of the packet tunnel. Genty et al further teaches each device has a set of several addresses (column 5, lines 34-41).

Claim 43 discloses the system of claim 35, wherein the source device and destination device establish the packet tunnel by establishing a first packet tunnel that terminates on an intermediate network device, and establishing a second packet tunnel that originates from the intermediate network device. Chen et al further teaches of the VPC must be concatenated to the destination links in order for the VCCs carried by VPC to be routed on the destination links to their destination, which forms a continuous

packet tunnel from multiple concatenated tunnels with intermediate devices (column 2, lines 10-18, and 23-28).

Claim 44 discloses the system of claim 43, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination device via the second packet tunnel. Genty et al further teaches of encapsulating a packet for transmission through a tunnel and using this encapsulation is widely known in the art (column 4, lines 9-15).

Claim 51 discloses a system comprising: a source network device that originates a first packet tunnel; an intermediate network device that terminates the first packet tunnel and originates a second packet tunnel; and a destination network device that terminates the second packet tunnel, wherein the intermediate network device de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination network device via the second packet tunnel. Genty et al teaches of a tunnel between a source and destination (figure 7) and encapsulating a packet for transmission through a tunnel and using this encapsulation is widely known in the art (column 4, lines 9-15). It fails to teach of an intermediate network device, which de-encapsulates packets received from the first packet tunnel and re-encapsulates the packets for communication to the destination network device via the second packet tunnel. Chen et al teaches of the VPC must be concatenated to the destination links in order for the VCCs carried by VPC to be routed on the destination links to their destination, which forms a continuous packet tunnel from

multiple concatenated tunnels with intermediate devices, when a new path is chosen the intermediate devices are redirect the data into the appropriate path (column 2, lines 10-18, and 23-28).

Genty et al and Chen et al are analogous art because they are both related to data protection over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the concatenation in Chen et al with the system in Genty et al because an improved protection architecture is provided for virtual connections in a network (Chen et al, column 1, lines 33-45).

Claim 52 discloses the system of claim 51, wherein the destination network device includes a storage medium to store a set of possible intermediate network devices, and further wherein the destination network device selects the intermediate network device from the set upon detecting a network attack. Genty et al further teaches of saving a list of addresses and selecting an address upon detection of a network attack (column 5, lines 34-41).

Claims 53 discloses a computer-readable medium comprising instructions to cause a processor to: establish a packet tunnel having a source network address and a destination network address; detect a network attack; select a new network address for at least one of the source network address and the destination network address upon detecting the network attack; and establish a new packet tunnel using the new network address, wherein the new packet tunnel comprises two or more concatenated packet tunnels. Genty et al teaches of a tunnel between a source and destination (figure 7), an

attack is detected (column 5, lines 48-52), a secondary tunnel can be established with different addresses (column 5, lines 63-67 – column 6, lines 1-6, 20-24), and a secondary tunnel is established (figure 7). It fails to teach of the new packet tunnel comprises two or more concatenated packet tunnels. Chen et al teaches of a virtual path connection (VPC) 38 which must be concatenated to the destination links in order for the virtual channel connections (VCCs) 36 carried by VPC 38 to be routed on the destination links to their destination, (figure 1, column 4, lines 8-21).

Genty et al and Chen et al are analogous art because they are both related to data protection over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the concatenation in Chen et al with the system in Genty et al because an improved protection architecture is provided for virtual connections in a network (Chen et al, column 1, lines 33-45).

Claim 56 discloses the computer-readable medium of claim 53, further comprising instructions to cause the processor to: select an intermediate network device; establish a first packet tunnel that terminates on the intermediate network device; and establish a second packet tunnel that originates from the intermediate network device. Chen et al further teaches of the VPC must be concatenated to the destination links in order for the VCCs carried by VPC to be routed on the destination links to their destination, which forms a continuous packet tunnel from multiple concatenated tunnels with intermediate devices, when a new path is chosen the

intermediate devices are inherently chosen during the route selection (column 2, lines 10-18, and 23-28).

Claims 5, 7, 9-11, 14, 15, 40, 54, and 55 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Chen et al (US Patent #6,353,593) as applied to claims 1, 27, 35, and 53 above, and further in view of Maeshima et al (US Patent #6,092,113).

Claim 5 discloses the method of claim 1, further comprising: reserving for the packet tunnel an amount of bandwidth within an access link coupled to a destination network device that terminates the packet tunnel; upon detecting the network attack, canceling the reserved bandwidth for the packet tunnel; and reserving for the new packet tunnel an amount of bandwidth within the access link. Genty et al in view of Chen et al teaches of the limitations of claim 1 as recited above and upon detecting a network attack canceling the bandwidth in a packet tunnel (Genty, column 6, lines 31-33). It fails to teach of reserving an amount of bandwidth for a packet tunnel and a replacement tunnel. Maeshima et al teaches of reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Chen et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 7 discloses the method of claim 1, further comprising: maintaining a set of available network addresses; selecting one of the network addresses as the new network address; establishing a new packet tunnel using the new network address for the destination address; and reserving for the new packet tunnel an amount of bandwidth within an access link. Genty et al in view of Chen et al teaches of the limitations of claim 1 as recited above, maintaining a set of available addresses, selecting an address as a net address and making a new tunnel (Genty et al, column 5, lines 34-41, 48-59, 63-67 – column 6, lines 1-6). It fails to teach of reserving bandwidth for the new tunnel. Maeshima et al teaches of reserving bandwidth for each tunnel on the network (column 3, lines 28-32).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Chen et al because bandwidth is assured in each tunnel (Maeshima, column 2, lines 8-10).

Claim 9 discloses the method of claim 8, further comprising: sending a message from a destination network device to a source network device instructing the source network device to establish the first packet tunnel with the intermediate network device; and reserving for the second packet tunnel an amount of bandwidth within an access link coupling the destination network device to a network. Genty et al in view of Chen et al teaches of the limitations of claim 8. It fails to teach of reserving a second amount of

bandwidth. Maeshima et al teaches of establishing a first tunnel with an intermediate device and the reservation of bandwidth for a second tunnel (figure 9A, column 4, lines 44-49, column 5, lines 28-36).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation and intermediate routers in Maeshima et al with the system in Genty et al in view of Chen because bandwidth is able to be allocated speedily and flexibly according to short term demand (Maeshima et al, column 3, lines 38-41).

Claim 10 discloses the method of claim 9, further comprising: establishing a secure signaling channel between the source network device and the destination network device; and sending the message via the secure signaling channel. Genty et al further teaches of a virtual private network as a secure connection and sending data over a secure channel (column 1, lines 19-25, figure 7).

Claim 11 discloses the method of claim 8, further comprising de-encapsulating at the intermediate network device packets received from the first packet tunnel; and re-encapsulating the packets at the intermediate network device for communication via the second packet tunnel. Genty et al further teaches of encapsulating a packet for transmission through a tunnel and using this encapsulation is widely known in the art (column 4, lines 9-15).

Claim 14 discloses the method of claim 5, wherein reserving an amount of bandwidth comprises sending a reservation message from a destination network device terminating the packet tunnel to a service provider access device. Maeshima further teaches of sending a message from a host (column 3, lines 28-32).

Claim 15 discloses the method of claim 14, wherein sending a reservation message comprises sending the reservation message according to the Resource Reservation Protocol (RSVP). Maeshima further teaches of using RSVP to reserve the bandwidth (column 3, lines 14-16).

Claim 40 discloses the system of claim 35, wherein the destination device reserves for the packet tunnel an amount of bandwidth within an access link coupling the network device to the network, and further wherein upon detecting the network attack the destination device cancels the reserved bandwidth for the packet tunnel and reserves the bandwidth for the new packet tunnel. Genty et al in view of Chen et al teaches of the limitations of claim 35 as recited above and upon detecting a network attack canceling the bandwidth in a packet tunnel (Genty et al, column 6, lines 31-33). It fails to teach of reserving an amount of bandwidth for a packet tunnel and a replacement tunnel. Maeshima et al teaches of reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in

Genty et al in view of Chen et al because it is possible to construct a VPN which enables assurance of bandwidth (Maeshima, column 3, lines 42-46).

Claim 54 discloses the computer-readable medium of claim 53, further comprising instructions to cause the processor to: reserve for the packet tunnel an amount of bandwidth within an access link; upon detecting the network attack, cancel the reserved bandwidth for the packet tunnel; and reserve an amount of bandwidth for the new packet tunnel. Genty et al in view of Chen et al teaches of the limitations of claim 53 as recited above and upon detecting a network attack canceling the bandwidth in a packet tunnel (column 6, lines 31-33). It fails to teach of reserving an amount of bandwidth for a packet tunnel and a replacement tunnel. Maeshima et al teaches of reserving bandwidth for every IP tunnel on the network (column 3, lines 1-23, 28-32).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Chen et al because it is possible to construct a VPN which enables assurance of bandwidth (column 3, lines 42-46).

Claim 55 discloses the computer-readable medium of claim 53, further comprising instructions to cause the processor to: maintain a set of available network addresses; select one of the network addresses as the new network address; establish a new packet tunnel using the new network address for the destination network address; and reserve for the new packet tunnel an amount of bandwidth within an

access link. Genty et al in view of Chen et al teaches of the limitations of claim 53 as recited above, maintaining a set of available addresses, selecting a address as a net address and making a new tunnel (Genty et al, column 5, lines 34-41, 48-59, 63-67 – column 6, lines 1-6). It fails to teach of reserving bandwidth for the new tunnel. Maeshima et al teaches of reserving bandwidth for each tunnel on the network (column 3, lines 28-32).

Genty et al in view of Chen et al and Maeshima et al are analogous art because they are related to virtual private network setup.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the bandwidth reservation in Maeshima et al with the system in Genty et al in view of Chen et al because bandwidth is assured in each tunnel (column 2, lines 8-10).

Claims 16, 17, and 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Chen et al (US Patent #6,353,593) as applied to claims 1 and 27 above, and further in view of Shawcross (US Patent #6,880,090).

Claim 16 discloses the method of claim 1, wherein establishing a packet tunnel comprises: maintaining a set of available multicast network addresses; selecting one of the multicast network addresses for the packet tunnel; and subscribing to a multicast channel for the selected multicast network address. Genty et al in view of Chen et al teaches of the limitations of claim 1 as recited above. It fails to teach of using multicast addresses. Shawcross teaches of maintaining a set of multicast addresses, selecting a

multicast address and subscribing to the multicast addresses (column 5, lines 60-67, column 6, lines 1-5).

Genty et al in view of Chen et al and Shawcross are analogous art because they are related to network attack prevention.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the multicast addressing in Shawcross with the system in Genty et al in view of Chen et al because the technique prevents unauthorized personnel from knowing which address to disrupt (Shawcross, column 6, lines 12-14).

Claim 17 discloses the method of claim 16, wherein establishing a new packet tunnel comprises: unsubscribing to the multicast channel; selecting one of the multicast network addresses for the destination network address; establishing a new packet tunnel using the new destination address; and subscribing to a multicast channel for the selected multicast network address. Shawcross further teaches of unsubscribing the multicast channel, selecting a multicast channel, establishing a new tunnel and subscribing to a multicast addresses (column 2, lines 62-67 – column 3, lines 1-17, column 9, lines 5-10, 36-42).

Claim 29 discloses the method of claim 27, wherein establishing a packet tunnel comprises: maintaining a set of available multicast network addresses; selecting one of the multicast network addresses for the destination network address of the packet tunnel; and subscribing to a multicast channel for the selected multicast network address. Genty et al in view of Chen et al teaches of the limitations of claim 27 as recited above. It fails to teach of using multicast addresses. Shawcross teaches of

maintaining a set of multicast addresses, selecting a multicast address and subscribing to the multicast addresses (column 5, lines 60-67, column 6, lines 1-5).

Genty et al in view of Chen et al and Shawcross are analogous art because they are related to network attack prevention.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the multicast addressing in Shawcross with the system in Genty et al in view of Chen et al because the technique prevents unauthorized personnel from knowing which address to disrupt (column 6, lines 12-14).

Claims 2 and 36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Chen et al (US Patent #6,353,593) as applied to claims 1 and 35 above, and further in view of Adams et al (US PGPUB US2003/0016679).

Claims 2 and 36 disclose the method and system of claims 1 and 35 wherein the source network address and the destination network address comprise port numbers. Genty et al in view of Chen et al teaches of the limitations of claims 1 and 35 as recited above. It fails to teach of the addresses comprising of port numbers. Adams et al teaches of control information being an IP address or a port number among other information (paragraph 21, lines 1-8).

Genty et al in view of Chen et al and Adams et al are analogous art because they are both related to routing data over a network.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the control information in Adams et al with the system in Genty et al

in view of Chen et al because the packet is able to be sent to its next destination once the information is known (Adams et al, paragraph 21, lines 8-12).

Claims 12, 13, 45, and 46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Genty et al (US Patent #6,473,863) in view of Chen et al (US Patent #6,353,593) as applied to claims 8 and 43 above, and further in view of Jorgensen (US PGPUB US2002/0099854).

Claim 12 discloses the method of claim 8, further comprising: establishing a secure signaling channel between a source network device and a destination network device; sending via the secure signaling channel control packets between the source network device and the destination network device to monitor the performance of the first and second packet tunnels; and selecting a new intermediate network device when the performance reaches a minimum threshold. Genty et al in view of Chen et al teaches of the limitations of claim 8 as recited above. It fails to teach of sending messages to monitor performance and making changes based on performance. Jorgensen teaches of monitoring, control, service, modify and repair a system by sending messages monitoring the performance and making changes based on performance (paragraph 612).

Genty et al in view of Chen et al and Jorgensen are analogous art because they are related to network setup and control.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring in Jorgensen with the system in Genty et al in view

of Chen et al because proactive provisioning of additional resources can occur (paragraph 612, lines 7-9).

Claim 13 discloses the method of claim 12, further comprising maintaining a set of possible intermediate network devices, and wherein selecting the intermediate network device comprises selecting one of the possible intermediate network devices from the set. Genty et al further teaches of each device has a set of several addresses, which are exchanged to each device, and the second device is selected from this list (column 5, lines 34-41).

Claim 45 discloses the system of claim 43, wherein the source device and the destination device establish a secure signaling channel and send via the secure signaling channel control packets to monitor the performance of the first and second packet tunnels. Genty et al in view of Chen et al teaches of the limitations of claim 43 as recited above. It fails to teach of monitoring performance. Jorgensen teaches of monitoring, control, service, modify and repair a system by sending messages monitoring the performance (paragraph 612).

Genty et al in view of Chen et al and Jorgensen are analogous art because they are related to network setup and control.

At the time of the invention it would have been obvious to a person of ordinary skill in the art to use the monitoring in Jorgensen with the system in Genty et al in view of Chen et al because proactive provisioning of additional resources can occur (paragraph 612, lines 7-9).

Claim 46 discloses the system of claim 45, wherein the destination device selects a new intermediate network device when the performance reaches a minimum threshold. Jorgensen further teaches of making changes based on the performance when monitoring (paragraph 612).

Response to Arguments

Applicant's arguments see remarks, page 13-20, filed November 28, 2005, with respect to the rejection(s) of claim(s) 1, 27, 35, 51, 53 under Genty et al in view of Maeshima et al have been fully considered and are persuasive. Therefore, the rejection has been withdrawn. However, upon further consideration, a new ground(s) of rejection is made in view of Chen et al.

Applicant asserts the prior art does not teach reserving an amount of bandwidth for the packet tunnel, canceling the reserved bandwidth upon detecting the network attack, and reserving an amount of bandwidth for the new packet tunnel in claims 5, 40, and 54. The Examiner respectfully disagrees, Genty et al teaches of the original tunnel may be abandoned inherently canceling the bandwidth involved in the tunnel (column 6, lines 31-33). Genty et al also teaches of detecting attacks (column 5, lines 48-59). Maeshima et al teaches of reserving bandwidth for every tunnel on the network, which includes the new tunnel (column 3, lines 1-23, 28-32).

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. Guruprasad (US PGPUB US2003/0076825) teaches of a self-scaling network, which allows concatenation of tunnels.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Brian J. Gillis whose telephone number is 571-272-7952. The examiner can normally be reached on M-F 7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Rupal Dharia can be reached on 571-272-3880. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Brian J Gillis
Examiner
Art Unit 2141

BJG

RUPAL DHARIA
SUPERVISORY PATENT EXAMINER